

Remarks

The Official Action rejected claims 1-34 and objected to the specification and claim 12. Applicant has amended the specification and claims 3, 10, 12 and 19. Claims 1-34 remain pending.

Specification Objections

The Official Action objected to informalities in paragraph [0001] of the present application. Applicant has amendment paragraph [0001] to address these informalities.

The Official Action further objected to the Abstract. In objecting to the Abstract, the Official Action indicates content that an abstract "should" contain and alleges the present Abstract must be corrected. However, Applicant respectfully points out that the allegedly missing content is merely "suggested" and not "required" as evidenced by the permissive word "should". Requirements are often prefaced with the words such as "must" or "shall". Applicant believes the Abstract satisfies all "requirements". If the Examiner elects to maintain the present objection, Applicant respectfully requests the Examiner to indicate which "requirements" the Abstract fails to satisfy.

Applicant respectfully requests the objections to the specification be withdrawn.

Claim Objectoins

Claim 12

The Official Action objected to claim 12 for informalities. Applicant has amended claim 12 to address these informalities. Applicant respectfully requests the objection of claim 12 be withdrawn.

Claims 32-33

The Official Action indicated that assuming claim 32 was allowed, claim 33 would be objected to under 37 CFR 1.75 as being a substantial duplicate thereof. As stated in MPEP 706.03(k):

[C]ourt decisions have confirmed applicant's right to restate (i.e., by plural claiming) the invention in a reasonable number of ways. ***Indeed, a mere difference in scope between claims has been held to be enough.*** (emphasis added).

Applicant respectfully points out that claims 32 and 33 do differ in scope. In particular, claim 32 is broader than claim 33 in that claim 32 permits the execution of one or more instructions to result in the computing device taking the stated actions. However, claim 33 requires execution of a launch instruction to result in the computing device taking the stated actions. Thus, claim 32 may encompass an embodiment not encompassed by claim 33. Applicant respectfully requests reconsideration.

Claim Rejections - 35 USC § 112

The Official Action rejected claim 3-5 and 10 under 35 USC §112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention.

In particular, claims 3-5 were rejected due to the use of the term "like a" in claim 3. Applicant has replaced the word "like" in claim 3 with the word "as" in order to address this rejection.

Further, claims 3-5 and 10 were rejected for lack of antecedent basis for the term "the processor" in claim 3 and claim 10. Applicant has amended claim 3 and claim 10. Applicant respectfully requests the present rejection of claims 3-5 and 10 be withdrawn in light of the present amendments.

Claim Rejections - 35 USC § 102

The Official Action rejected claims 1-2 and 6-34 under 35 USC 102(e) as being anticipated by Davis et al (US 6,401,208). Applicant respectfully requests the rejection of claims 1-2 and 6-34 be withdrawn in light of the following.

Claims 1-2, 6-9, 12-13 and 29-34

Claims 1-2, 6-9, 12-13 and 29-34 require transferring an authenticated code module to a private memory and executing the authenticated code module ***stored in the private memory*** in response to determining that the authenticated coded module stored in the private memory is authentic.

Davis appears to disclose transferring BIOS code from a BIOS device 170₁ to a cryptographic device 410 (Davis, col. 5, lines 55-65). Davis further appears to disclose authenticating the received BIOS code (Davis, col. 5, line 66 through col. 6, line 13). However, Davis appears to teach executing the authenticated BIOS code from the BIOS device 170₁ instead of a private memory as required by claim 1 (Davis, col. 6, lines 20-30). As a result, Davis is susceptible to an attack which changes the BIOS code stored in the BIOS device 170₁ after the cryptographic device 410 determined the BIOS code was authentic. While the window between

when the cryptographic device 410 determines the BIOS code is authentic and when the processor completes execution of the BIOS code may be small, there is still a chance for an attacker to change the BIOS code during this window and thus compromise the system.

The invention of claims 1-2, 6-9, 12-13 and 29-34 may thwart such an attack by transferring the authenticated code module to a private memory and executing the authenticated code module from the private memory. Since the Davis does not appear to teach transferring the authenticated code module to a private memory and executing the authenticated code module from the private memory, Davis does not anticipate claim 1-2, 6-9, 12-13 and 29-34. Applicant respectfully requests the rejection of claims 1-2, 6-9, 12-13 and 29-34 be withdrawn.

Claim 10

Claim 10 includes claim 1 as a base claim. Accordingly, claim 10 is allowable for at least reasons similar to those stated above in regard to claim 1. Furthermore, claim 10 as amended requires retrieving the key from a processor used to execute the authenticated code module. Col. 5, line 65 though col. 6, line 13 of Davis appear to disclose a root certificate key 527 of the cryptographic device 410 and a public key from a BIOS certificate 181 of the BIOS device 170₁. Neither the cryptographic device 410 nor the BIOS device 170₁ appear to execute the BIOS code. Davis appears to teach that only the processing unit 110 executes the BIOS code that is authenticated by the cryptographic device 410 (Davis, col. 6, lines 20-30); however, Davis is silent regarding retrieving a key from the processing unit 110. Accordingly, Davis does not appear to teach retrieving the key from a processor used to execute

the authenticated code module as required by claim 10. Applicant respectfully requests the rejection of claim 10 be withdrawn.

Claim 11

Claim 11 includes claim 1 as a base claim. Accordingly, claim 11 is allowable for at least reasons similar to those stated above in regard to claim 1. Furthermore, claim 11 requires retrieving the key from a chipset. The Official Action appears to rely on Davis col. 4, line 15-27 for such a teaching. However, Davis in the identified section appears to indicate that the processing unit 110, chipset 130, and cryptographic device 410 may be mounted to system substrate 210. Applicant believes this is merely indicating that a system substrate 210 such as a mainboard or motherboard may be populated with a processing unit 110, a chipset 130 and a cryptographic device 410. Applicant has been unable to locate any teaching in Davis of the chipset having a key which may be retrieved. Since Davis does not appear to teach retrieving the key from a chipset, Davis does not anticipate claim 11. Applicant respectfully requests the rejection of claim 11 be withdrawn.

Claims 14-15 and 17-18

Claims 14-15 and 17-18 require a private memory coupled to a chipset, and a processor to transfer an authenticated code module from a machine readable medium to the private memory and to authenticate the authenticated code module stored in the private memory. The only memory Davis appears to disclose that is coupled to the chipset 130 is main memory 120 (Davis, FIG. 1). However, Davis does not appear to transfer the BIOS code 180 from the BIOS device 170₁ to main memory 120. Instead, Davis appears to teach transferring the BIOS code 180 to the cryptographic device 410 (Davis, col. 5, lines 55-65). Accordingly, Davis does not

appear to teach transferring an authenticated code module to a private memory coupled to a chipset as required by claims 14-15 and 17-18.

Furthermore, Davis appears to teach that the processing unit 110 transfers the BIOS code 180 to the cryptographic device 410 (Davis, col. 5, lines 55-65) and that the cryptographic device 410 authenticates the BIOS code 180 (Davis, col. 5, line 65 through col. 6, line 13). Accordingly, Davis does not appear to teach a processor that both transfers the authenticated code module and authenticates the authenticated code module as required by claims 14-15 and 17-18.

Since Davis does not appear to teach a private memory coupled to a chipset, and a processor to transfer an authenticated code module from a machine readable medium to the private memory and to authenticate the authenticated code module stored in the private memory as required by claims 14-15 and 17-18, Applicant respectfully requests the rejection of claims 14-15 and 17-18 by withdrawn.

Claim 16

Claim 16 includes claim 14 as a base claim. Accordingly, claim 16 is allowable for at least reasons similar to those stated above in regard to claim 14. Furthermore, claim 16 requires the chipset to comprise a key. Thus, claim 16 is allowable for reasons similar to the above reasons stated for claim 11. Applicant respectfully requests the rejection of claim 16 be withdrawn.

Claims 19-21

Claims 19-21 require a processor to authenticate the authenticated code module stored in the private memory, and to execute the authenticated code module stored in the private memory after authenticating the authenticated code module.

Claims 19-21 are allowable for reasons similar to those stated in regard to claim 1.

Applicant respectfully requests the rejection of claims 19-21 be withdrawn.

Claim 22

Claim 22 includes claim 19 as a base claim. Accordingly, claim 22 is allowable for at least reasons similar to those stated above in regard to claim 19. Claim 22 further requires the private memory to comprise the internal cache memory of the processor. The Official Action appears to rely on the internal memory 525 for such a teaching. However, the internal memory 525 does not appear to be a **cache** memory as required by claim 22. At col. 4, lines 41-59, Davis teaches that the internal memory 525 is a non-volatile memory such as ROM, EPROM, or EEPROM which are not suitable for implementing a cache memory. Applicant respectfully requests the rejection of claim 22 be withdrawn.

Claim 23

Claim 23 includes claim 19 as a base claim. Accordingly, claim 23 is allowable for at least reasons similar to those stated above in regard to claim 19. Claim 23 further requires other processors coupled to a processor bus and the processor to lock the processor bus to prevent the other processors from altering the authenticated code module. The Official Action points to Davis, col. 4, lines 1-27 for such a teaching. While Davis in the cited section may disclose a processing unit 110 and a cryptographic device 410 connected to the processing unit 110 via a dedicated processor bus 420, there appears to be no teaching of **locking** the processor bus 420 to prevent other processors from altering the authenticated code module as required by claim 23. Applicant respectfully requests the rejection of claim 23 be withdrawn.

Claims 24 and 27-28

Claims 24 and 27-28 require a chipset comprising a memory control that defines a portion of a memory as private memory. While Davis may disclose a system memory 120 and a chipset 130, Applicant has been unable to locate any teaching regarding the chipset 130 defining a portion of the system memory 120 as private memory. Applicant respectfully requests the rejection of claims 24 and 27-28 be withdrawn.

Claim 25

Claim 25 includes claim 24 as a base claim. Accordingly, claim 25 is allowable for at least reasons similar to those stated above in regard to claim 24. Claim 25 further requires the chipset to comprise a memory controller coupled to the memory and a separate private memory controller coupled to the private memory. While Davis may disclose a chipset 130 to interface the system memory 120 and a cryptographic device 410 with internal memory 525, Davis appears to provide no teaching regarding a chipset 130 that has two memory controllers has required by claim 25. Applicant respectfully requests the rejection of claim 25 be withdrawn.

Claim 26

Claim 26 includes claim 24 as a base claim. Accordingly, claim 26 is allowable for at least reasons similar to those stated above in regard to claim 24. Furthermore, claim 26 requires the chipset to comprise a key. Thus, claim 26 is allowable for reasons similar to the above reasons stated for claim 11. Applicant respectfully requests the rejection of claim 26 be withdrawn.

Conclusion

The foregoing is submitted as a full and complete response to the Official Action. Applicant submits that all remaining claims are in condition for allowance. Reconsideration is requested, and allowance of all remaining claims is earnestly solicited.

Should it be determined that an additional fee is due under 37 CFR §§1.16 or 1.17, or any excess fee has been received, please charge that fee or credit the amount of overcharge to deposit account #02-2666. If the Examiner believes that there are any informalities which can be corrected by an Examiner's amendment, a telephone call to the undersigned at (503) 439-8778 is respectfully solicited.

Respectfully submitted,



Gregory D. Caldwell
Reg. No. 39,926

Date: January 6, 2006

Blakely, Sokoloff, Taylor & Zafman, LLP
1279 Oakmead Parkway
Sunnyvale, CA 94085-4040
(408) 720-8300

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to:
Commissioner for Patents, P.O. Box 1450 Alexandria, VA 22313-1450

On: January 6, 2006

Signature:



Katherine Jennings